1. A method of implementing token-based electronic security across multiple secure web sites, in which the user has a security token, comprising:

storing unique token identification information, and the seed value of each token, in a security system;

requiring the user, upon login to a secure web site, to enter at least the code generated by the user's token;

passing the user's token code from the web site to the security system;

using the security system to verify whether or not the user's token code was generated by the user's token; and

passing the verification information from the security system to the web site, for use in web site security.

2. The method of claim 1 wherein the requiring step further requires the user to enter a user name and user password.

3. The method of claim 2 further comprising the step of:

the web site verifying the user name and user password before passing the user's token code to the security system.

4. A method of accomplishing two-factor user authentication, comprising:

providing two separate user authentication methods;

enabling a user to communicate authentication data for both authentication methods to a first web site using the internet;

enabling the communication of at least some of the authentication data from the first web site to a second web site using the internet; and

wherein both web sites are involved in user authentication using the authentication data.

5. The method of claim 4, wherein the first web site initially authenticates the user based on the data relating to one of the authentication methods.

6. The method of claim 5, wherein the second web site completes user authentication based on the data relating to the other authentication method.

7. The method of claim 6, wherein the first web site communicates with the second web site only if the user is initially authenticated.

8. The method of claim 7, wherein the first web site communicates to the second web site at least data relating to the other authentication method, and user-identification data.

9. The method of claim 4, wherein one authentication method employs a password.

10. The method of claim 4, wherein one authentication method employs a token.

11. The method of claim 10, wherein the token is hardware-based, and generates a code that comprises at least some of the data for the authentication method.

12. The method of claim 11, wherein the token is a stand-alone, portable device.

13. The method of claim 11, wherein the token is USB-based and is accessed by a browser.

14. The method of claim 10, wherein the token is software-based, and generates a code that comprises at least some of the data for the authentication method.

15. The method of claim 14, wherein the token comprises a browser plug-in.

16. The method of claim 4, wherein one authentication method employs a fixed complex code.

17. The method of claim 16, wherein the fixed complex code comprises a public key infrastructure.

18. The method of claim 4, wherein one authentication method is software-based.

19. The method of claim 4, wherein at least one user authentication method can be used across multiple web sites.

20. The method of claim 10, wherein the token is embedded in a device such as a cell phone.